Microsoft

Operating System

Using Secondary Logon (Run As) in Windows 2000

Beta 3 Technical Walkthrough

Abstract

This technical walkthrough provides examples of using the secondary logon feature in the Microsoft® Windows® 2000 operating system. Secondary logon (Run As) allows administrators to avoid having to log on with an administrative account for each task. Instead, secondary logon enables administrators to log on with an ordinary user account and then start trusted administrative tools in the context of the administrator's account without logging off. This feature can be used by any user with multiple credentials to start applications under different credentials without needing to log off.

© 1999 Microsoft Corporation. All rights reserved.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This BETA document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

0599

CONTENTS

INTRODUCTION

Until now, one of the biggest problems with respect to security has been that administrators always log on to the administrator account and perform privileged as well as nonprivileged operations from the same logon session. This is primarily because it is far more convenient to log on once and complete all of the operations needed than it is to constantly log on and off based on the task being performed. This makes computers running the Microsoft® Windows NT® operating system susceptible to *Trojan horse* attacks. The simple act of running Internet Explorer and accessing a nontrusted Web site can be extremely damaging to the system if done from an administrative context. The Web page may have Trojan horse code that can be downloaded to the system and then executed in the administrative context. This code could perform such tasks as reformatting a disk, deleting all files, creating a new user with administrative access, and so on.

The secondary logon capability in the Microsoft Windows® 2000 operating system addresses this problem by providing a way to start applications in different security contexts without having to log off. This capability is provided using the Secondary Logon Service and the feature is referred to as *Run As*.

Secondary logon allows administrators to log on to a non-administrative account and still be able to perform administrative tasks by running trusted administrative applications in an administrative context. Secondary logon requires system administrators to have two user accounts: a regular account that has basic user rights and security, and an administrative account that can be different for each administrator or shared among administrators.

Even though this feature is primarily intended for system administrators to separate administrative operations from normal operations, it can be used by any user with multiple accounts to start applications under the different account contexts without needing to log off.

This technical walkthrough introduces you to the secondary logon feature and its associated tools using different examples.

USING SECONDARY LOGON FEATURES

Activating the Secondary Logon Feature

The Secondary Logon Service starts automatically after a clean install of Windows 2000. However, if this service is not currently running, use the following steps to start the service.

To start the Secondary Logon Service

1. Log on using an account with administrative privileges.
2. Right-click **My Computer** and click **Manage**.
3. Under **Computer Management**, click **System Tools**, and then click **Services**.

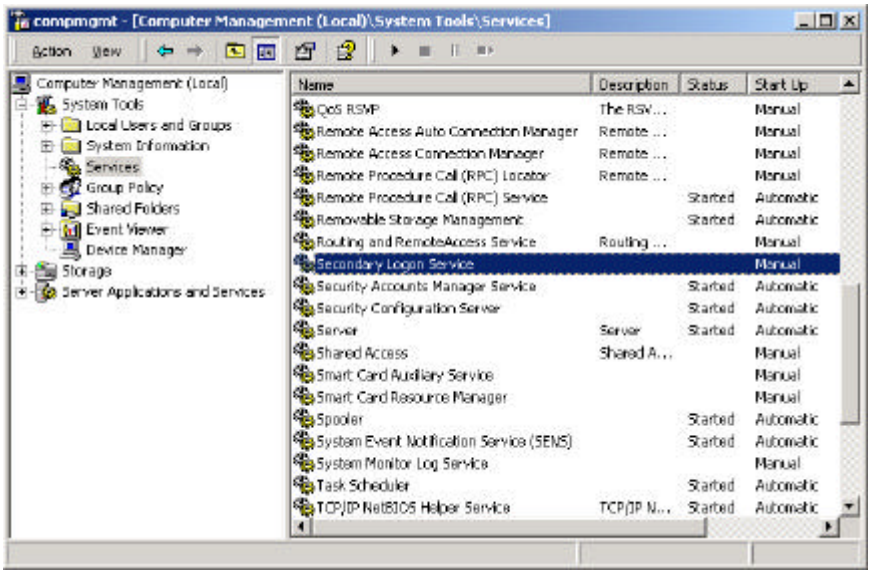

Figure 1. Select the Secondary Logon Service

4. Double-click **Secondary Logon Service**. The **Properties on Local** dialog box appears.

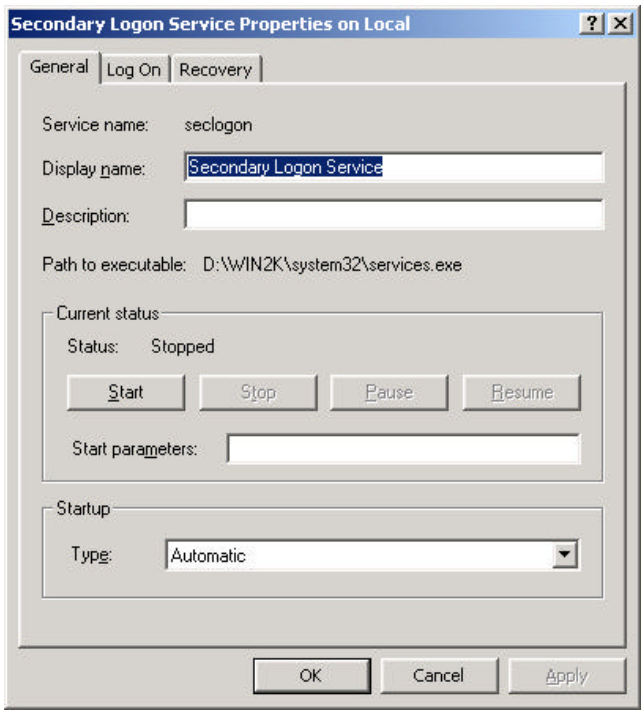

Figure 2. Secondary Logon Service Properties on the local computer

5. Set the **Startup** mode to **Automatic** so that you do not have to restart this service each time you reboot.
6. Click the **Start** button to use the service immediately. Click **OK** to close the **Properties** dialog box.

Using Secondary Logon with a Normal User Account

Before performing these steps, create an ordinary user account named *JoeUser*, using **Local Users and Groups** (on workstations and stand-alone servers) or the **Active Directory Users and Groups** tool (on a domain controller). For this walkthrough, you can use the default administrator account as the administrative account.

After you create the account, log off of the administrator account and log on using the ordinary user account.

To use secondary logon to start the Add/Remove Hardware tool

1. From the **Start** menu, point to **Settings**, and then click **Control Panel**.
2. Try to start the **Add/Remove Hardware** tool by double-clicking the icon. Because you are running in a normal user security context, you should receive an error message explaining that you do not have sufficient privileges to start this tool. Click **OK** to close this dialog box.
3. Select the **Add/Remove Hardware** tool by using a single left-click on the icon.

4. Hold down the Shift key and right-click the Add/Remove Hardware icon. Note the **Run as** option appears on the menu.

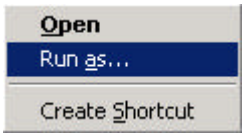

Figure 3. Run as option

5. Click **Run as**. The **Run program as other user** dialog box appears.

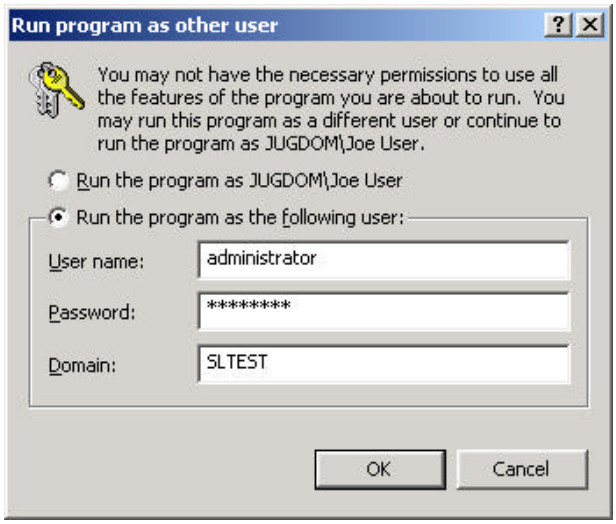

Figure 4. Run program as other user

6. Type the administrator name and password in the appropriate fields. Note that the domain name can also be changed. Click **OK**.
7. The Add/Remove Hardware wizard starts. Click the **Cancel** button to close the wizard.

To use an .msc file to start a Microsoft Management Console (MMC)

Note This example uses an existing MSC file, Diskmgmt.msc, but any .msc file can be started in a different security context using this method.

1. Using Windows Explorer, copy the file Diskmgmt.msc to your desktop. Diskmgmt.msc can be found in the %WINDIR%\SYSTEM32 subdirectory. By default, this directory is \WINNT\SYSTEM32, located on the boot partition.
2. Use a single click to select the file on your desktop.
3. Hold down the Shift key, and right-click the Diskmgmt icon.

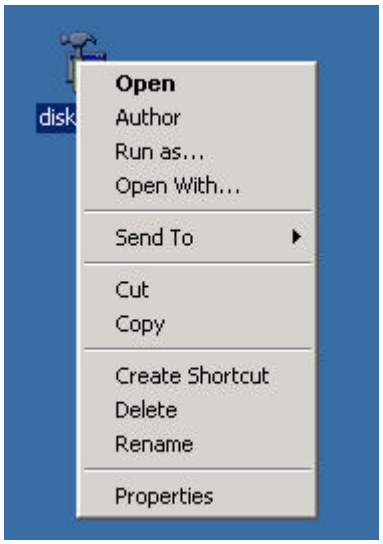

Figure 5. Using Run As from an .msc file

4. Select the **Run as** command. The **Run program as other user** dialog box appears.
5. Type the administrator name and password in the appropriate fields. Click **OK**. A new MMC console appears with the Disk Management snap-in loaded.

This snap-in is now running in administrative context. In most cases, system administrators will want to create custom MMC consoles that contain frequently used administrative snap-ins, and then run them using secondary logon.

To start an application in an administrative context

Note This example uses the Notepad application, but you can open any Windows application in an alternate security context using this method.

1. Using Windows Explorer, copy the file Notepad.exe to your desktop. Notepad. Exe can be found in the \%WINDIR%\ directory. By default, this directory is \WINNT\ located on the boot partition.
2. Click the Notepad icon on the desktop.
3. Hold down the Shift key and right-click the Notepad icon.
4. Select the **Run As** command. The **Run program as other user** dialog box appears.
5. Type the administrator name and password in the appropriate fields. Click **OK**. Notepad should now start up.

Note There is no indication of which security context this application is running in. This is because Windows applications define their own title text that cannot be manipulated by the caller. This may cause some confusion if you start up multiple processes in different contexts.

To start a shortcut in an administrative context

Note The following method will work on shortcuts of .exe files and shortcuts of registered file types, such as .txt, .doc, and .msc.

1. Create a shortcut to the Diskmgmt program that you created in the previous example: right-click the Diskmgmt icon, and then click **Create Shortcut**.
2. Use a single left click to select the shortcut to Diskmgmt icon on your desktop.
3. Hold down the Shift key. and right-click the shortcut to Diskmgmt icon.

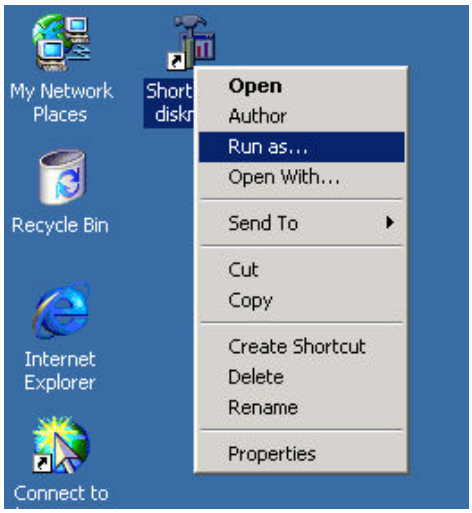

Figure 6. Select the shortcut to Diskmgmt

4. Select the **Run as** command. The **Run program as other user** dialog box appears.
5. Type the administrator name and password in the appropriate fields. Click OK. This will launch another MMC console with the Disk Management snap-in loaded.

You can also configure a shortcut to always use alternate credentials when the shortcut is opened.

To configure this option

1. Close any open MMC consoles.
2. Select the Shortcut to Diskmgmt icon.
3. Right-click the icon, and select **Properties**.
4. Select the **Run as different user** check box.

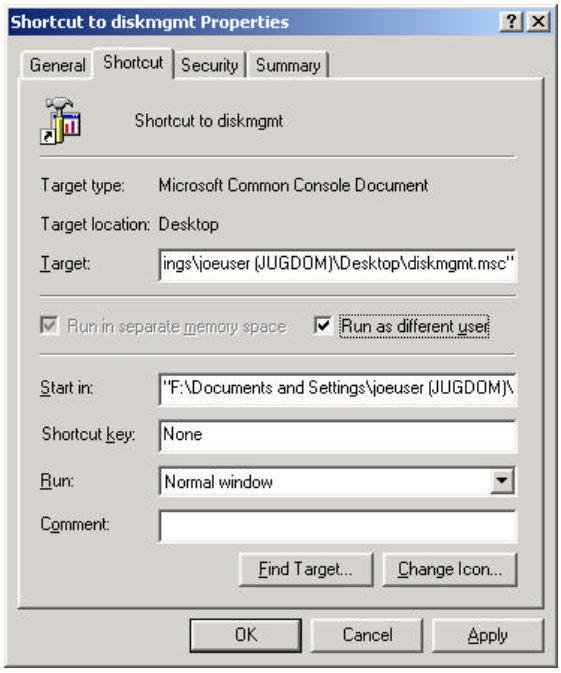

Figure 7. Configure shortcut credentials

5. Click **OK** to close the **Properties** dialog box.
6. Double-click the Shortcut to Diskmgmt icon to open the console.
7. The **Run program as other user** dialog box appears. Complete the appropriate fields, and click the **OK** button.

This technique can be used for any shortcuts that you create and always need to run under a different security context.

To start a command prompt in the local computer administrative context

1. From the **Start** menu, click **Run**.
2. Type

   `runas /user:<machine name>\administrator cmd`

   where <*machine name*> is the name of your computer.
3. Click **OK**.

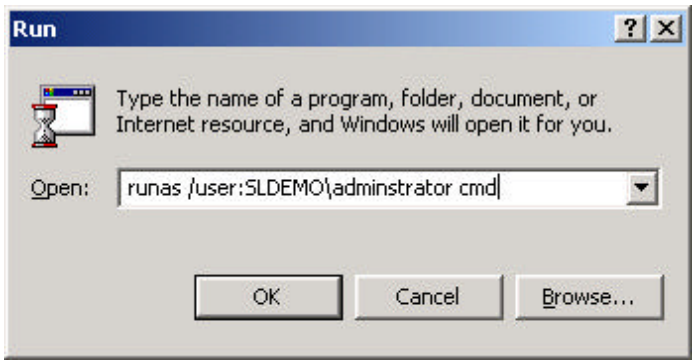

Figure 8. Start a command prompt in the administrative context

4. A console window appears to prompt you for the password for the ***<machine name>*\administrator** account. Type the password, and then press Enter.
5. A new console window starts, running in the administrative context. The title of the console will clearly state **running as *<machine name>*\administrator**. You can now start any command-based administrative programs from this console window.

Running Secondary Logon Using Other Security Contexts

The previous examples show the use of secondary logon to run administrative tools in an administrative context. The feature does not preclude starting applications and tools in other security contexts, some of which may have limited capabilities. The feature is general enough to allow running any application or tool in any security context as long as:

- You can provide the appropriate account credentials for the alternate context.
- The alternate context has the ability to log on locally to the system.
- The application or tool is available on the system and is accessible to the alternate context.

Limitations and Workarounds

If you attempt the examples above and the results are not as expected, one of the following workarounds may be able to resolve the issue.

- Secondary Logon Service is not started. Refer to the section “Activating the Secondary Logon Feature,” to start the service.
- The credentials supplied may not be correct. Verify the credentials by logging off and logging on as that user from the initial Windows log on screen. If the logon fails because of a bad password or because the account used doesn’t have access to the current system, then secondary logon will have the same security constraints.
- An .exe will not start. You might be trying to start an .exe from a network path but the credentials used to connect to the network path are not the same as the one being used to start the .exe. The credentials used to start the .exe may not

have access to the network path. First start the Windows 2000 command prompt using Run as, then use the Net Use command to reconnect to the network path, and then start the .exe.

- Certain applications are launched indirectly by the shell. This includes tools such as Control Panel, the Printers utility, and so on. Because the shell is started in the primary security context during initial logon, any process launched from the shell remains in that security context. Either start the application using the **Run as** menu option discussed above or to shut down the existing shell and restart it in the administrative security context, as explained next.

To run the Explorer shell in an administrative security context

1. Start **Task Manager**. Right-click the **Task** bar, and then click **Task Manager**.
2. Click the **Processes** tab.

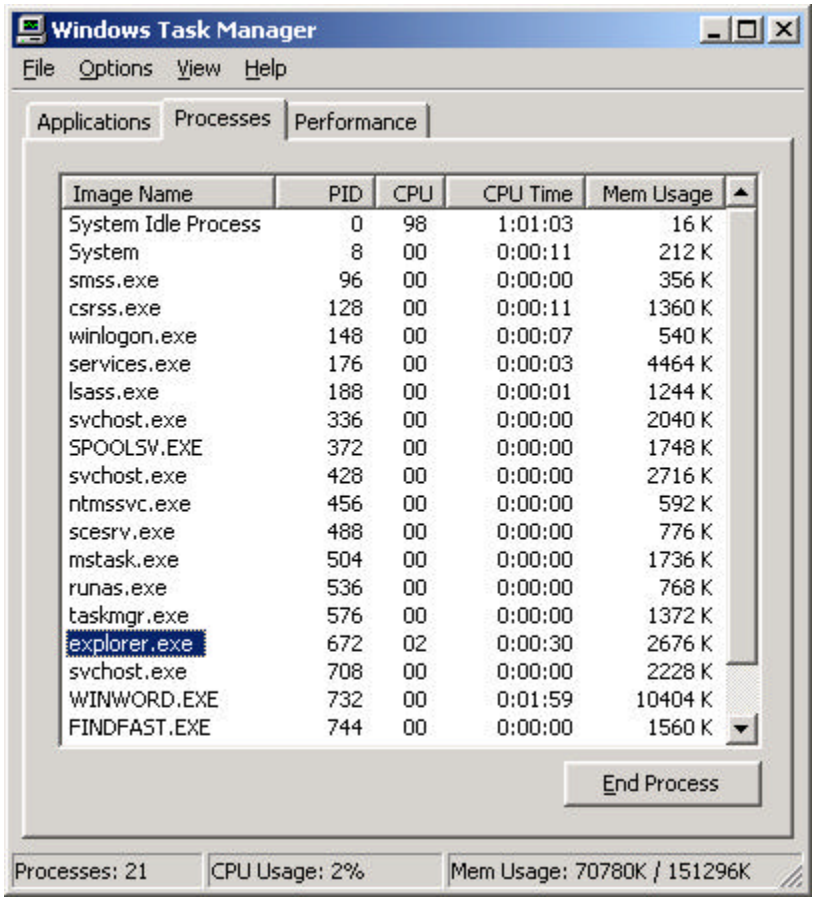

Figure 9. Use Task Manager to stop the Explorer

3. Select **Explorer.exe**, and then click **End Process**.

4. Click **Yes** on the warning pop-up message. The entire desktop disappears, however, any applications that you have started are still running (including Task Manager).

5. Click the **Applications** tab.

6. Click **New Task**.

7. Type

```
runas /user:<machine/domain name>\administrator explorer.exe
```

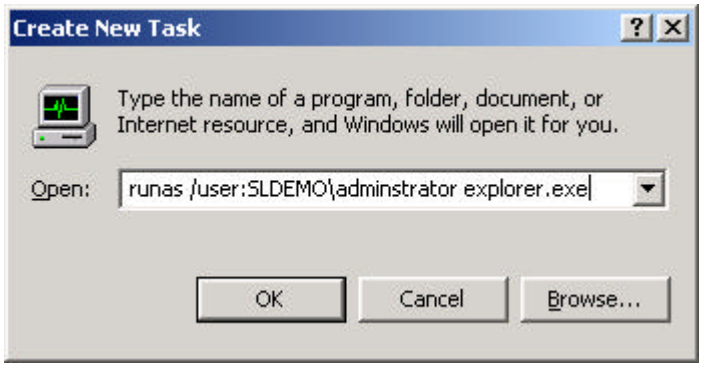

Figure 10. Create a new task

8. Click **OK**.

9. A console window appears and prompts for the password. Minimize Task Manager, type the **password**, and press Enter.

10. The desktop returns, including the task bar, shortcuts, Startup folder items, and so on. Perform any required administrative tasks. For example, from the **Start** menu, click **Settings**, and then click **Control Panel**. This starts up the Control Panel in an administrative context.

11. When you are finished, log off of the administrator account. A new shell should automatically start, running in the original JoeUser user context.

FOR MORE INFORMATION

For the latest information on Microsoft Windows 2000 network operating system, visit our World Wide Web site at http://www.microsoft.com/windows/server/ and the Windows NT Server Forum on the Microsoft Network (GO WORD: MSNTS).

For the latest information on the Windows 2000 Beta 3, visit the World Wide Web site at http://ntbeta.microsoft.com.

Before You Call for Support

Please keep in mind that Microsoft does not support these walkthroughs. The purpose of the walkthroughs is to facilitate your initial evaluation of the Microsoft Windows 2000 features. For this reason, Microsoft cannot respond to questions you might have regarding specific steps and instructions.

Reporting Problems

Problems with Microsoft Windows 2000 Beta 3 should be reported through the appropriate bug reporting channel and alias. Please make sure to adequately describe the problem so that the testers and developers can reproduce and fix it. Refer to the Release Notes included on the Windows 2000 Beta 3 distribution media for some of the known issues.